IN THE CLAIMS

The following is a complete listing of the claims, and replaces all earlier versions and listings.

1. (Currently Amended) A method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

[[-]] segmenting [[(E2)]] the data into regions; and

[[-]] associating [[(E3)]] at least one region with each symbol to be inserted, wherein, for each region into which a symbol in question is to be inserted, said associating step includes the steps of:

[[-]] determining [[(E7)]] a pseudo-random function, from a key which depends on an initial key and on a length of the message,

[[-]] modulating [[(E8)]] the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

[[-]] adding [[(E10)]] the pseudo-random sequence to a region in question.

2. (Currently Amended) A method according to Claim 1, wherein a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

[[-]] a number of times the symbol to be inserted has already been inserted into other regions, and

[[-]] a ranking of the symbol among the ordered symbols.

3. (Currently Amended) A method according to Claim 1 or 2, further comprising the step of transforming [[(E1)]] the digital data by a reversible transformation.

4. (Currently Amended) A method for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

[[-]] segmenting ~~(E210)~~ the data into regions;

[[-]] extracting [[(E21)]] a length of an inserted message; and

[[-]] extracting [[(E22)]] the inserted message.

5. (Currently Amended) A method according to Claim 4, wherein said step of extracting the length of the inserted message includes the steps of:

[[-]] selecting ~~(E211)~~ a set of length values; [[,]]

[[-]] calculating ~~(E217)~~ a correlation value between the message and the digital data, for each of the length values; [[,]] and

[[-]] determining ~~(E223)~~ a local maximum among the correlation values.

6. (Previously Presented) A method according to Claim 4 or 5, wherein said step of extracting the length of the inserted message is carried out while processing F times fewer coefficients than included in the digital data.

7. (Currently Amended) A method according to Claim 6, further comprising the steps of:

[[-]] determining [[(E22)]] a total number of coefficients [[(C)]] to be considered;

[[-]] selecting ~~(E26, E27)~~ a maximum number of coefficients corresponding to a same inserted symbol, and, if the total number of coefficients to be considered has not been reached,

[[-]] reiterating [[(E29)]] said selecting step, for another symbol.

8. (Currently Amended) A device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, said device comprising:

[[-]] means [[(3)]] for segmenting the data into regions; and

[[-]] means [[(5)]] for associating at least one region with each symbol to be inserted,

wherein said means for associating includes:

[[-]] means [[(7)]] for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

[[-]] means [[(8)]] for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

[[-]] means [[(5)]] for adding the pseudo-random sequence to a region in question.

9. (Currently Amended) A device according to Claim 8, wherein said means [[(7)]] for determining a pseudo-random function is configured in such a way that a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

[[-]] a number of times the symbol to be inserted has already been inserted into other regions, and

[[-]] a ranking of the symbol among the ordered symbols.

10. (Currently Amended) A device according to Claim 8 or 9, further comprising means [[(2)]] for prior transformation of the digital data by a reversible transformation.

11. (Currently Amended) A device for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said device comprising:

[[-]] means for segmenting the data into regions;

[[-]] means [[(22)]] for extracting a length of the inserted message; and

[[-]] means (23) for extracting the inserted message.

12. (Currently Amended) A device according to Claim 11, wherein said means [[(22)]] for extracting the length of the inserted message includes:

[[-]] means for selecting a set of length values,

[[-]] means for calculating a correlation value between the message and the digital data, for each of the length values, and

[[-]] means for determining a local maximum from among the correlation values.

13. (Previously Presented) A device according to Claim 11 or 12, wherein said means for extracting the length of the inserted message is configured to perform extraction while processing F times fewer coefficients than included in the digital data.

14. (Currently Amended) A device according to Claim 13, further comprising:

[[-]] means for determining a total number of coefficients [[(C)]] to be considered;

[[-]] means for selecting a maximum number of coefficients corresponding to a same inserted symbol; and

[[-]] means for reiterating processing of said means for selecting, for another symbol, if the total number of coefficients to be considered has not been reached.

15. (Currently Amended) A device according to Claim 8, wherein said steps of segmenting and associating, and the steps of determining, modulating, and adding are performed by:

[[-]] a microprocessor [[(100)]],

[[-]] a read-only memory [[(102)]] including a program for processing the data, and

[[-]] a random-access memory [[(103)]] including registers suitable for recording variables modified during running of the program.

16. (Currently Amended) A device according to Claim 11, wherein said means for segmenting and said means for extracting are incorporated into:

[[-]] a microprocessor [[(100)]],

[[-]] a read-only memory [[(102)]] including a program for processing the data, and

[[-]] a random-access memory [[(103)]] including registers suitable for recording variables modified during running of the program.

17. (Currently Amended) An apparatus [[(10)]] for processing a digital image, comprising means suitable for implementing the method according to any one of claims 1 and 4.

18. (Currently Amended) An apparatus [[(10)]] for processing a digital image, comprising a device according to any one of claims 8 and 11.

19. (Previously Presented) A storage medium storing a computer-readable program for implementing a method for inserting according to Claim 1.

20. (Currently Amended) A storage medium according to Claim 19,

wherein said storage medium is detachably mountable on a device for inserting a message that includes ordered symbols into digital data representative of physical quantities, and

wherein the device comprises:

[[-]] means [[(3)]] for segmenting the data into regions;

[[-]] means [[(5)]] for associating at least one region with each symbol to be inserted, [[the]] <u>said</u> means for associating including:

[[-]] means [[(7)]] for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

[[-]] means [[(8)]] for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

[[-]] means [[(5)]] for adding the pseudo-random sequence to a region in question.

21. (Previously Presented) A storage medium according to Claim 19, wherein said storage medium is a floppy disk or a CD-ROM.

22. (Previously Presented) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method of inserting according to Claim 1.

23. (Previously Presented) A storage medium storing a computer-readable program for implementing a method of extracting according to Claim 4.

24. (Currently Amended) A storage medium according to Claim 23, wherein said storage medium is detachably mountable on a device for extracting a message

that includes ordered symbols from digital data representative of physical quantities, the device comprising:

[[-]] means for segmenting the data into regions;

[[-]] means [[(22)]] for extracting a length of the inserted message; and

[[-]] means [[(23)]] for extracting the inserted message.

25. (Previously Presented) A storage medium according to Claim 23, wherein said storage medium is a floppy disk or a CD-ROM.

26. (Previously Presented) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method for extracting according to Claim 4.